(51) International Patent Classification⁷: G06F 1/00

(21) International Application Number: PCT/US01/11907

(22) International Filing Date: 11 April 2001 (11.04.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/547,183   11 April 2000 (11.04.2000)   US

(71) Applicant: SUN MICROSYSTEMS, INC. [US/US]; 901 San Antonio Road, MS PAL1-521, Palo Alto, CA 94303 (US).

(72) Inventors: ELLEY, Yassir, K.; 664 B South Street, Waltham, MA 02453 (US). ANDERSON, Anne, H.; 28 Minuteman Road, Acton, MA 01720 (US). HANNA, Stephen, R.; 3 Beverly Road, Bedford, MA 01730 (US). MULLAN, Sean, J.; 102 Ashbrook, Howth Road, Clontarf, Dublin 3 (IE). PERLMAN, Radia, Joy; 10 Huckleberry Lane, Acton, MA 01720 (US).
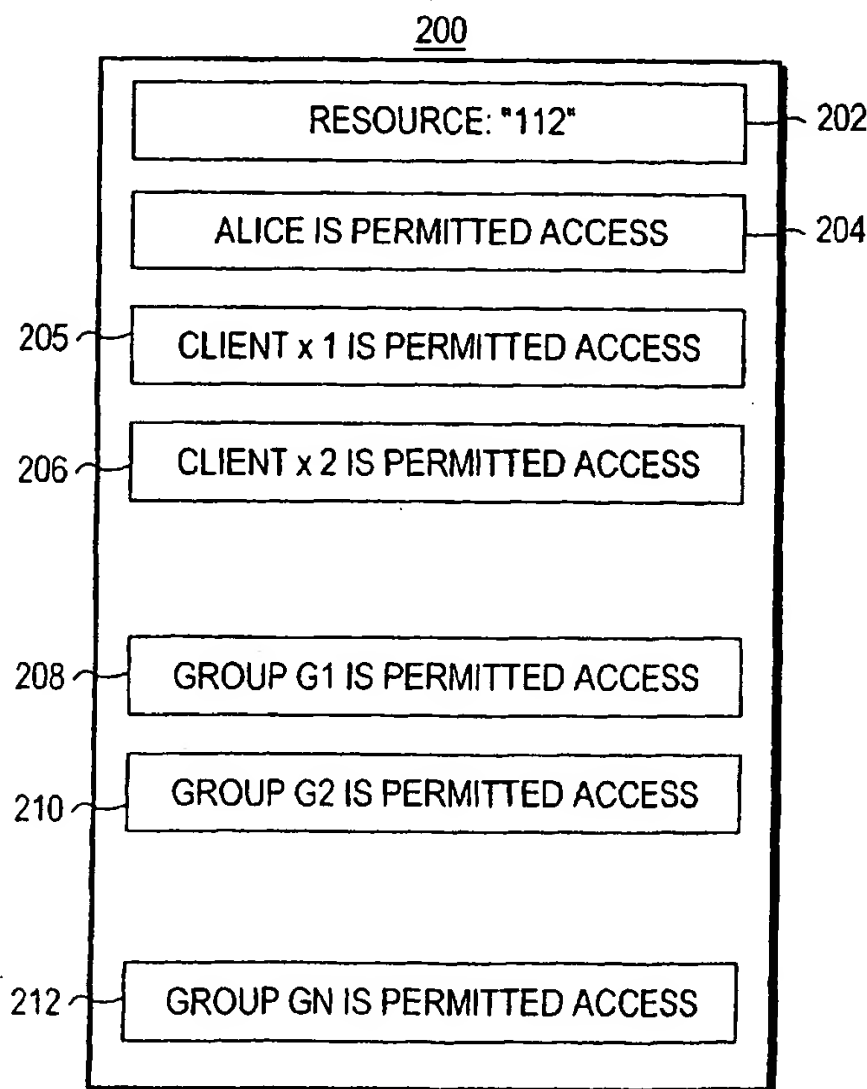
(74) Agents: CESARI, Robert, A. et al.; Cesari and McKenna, LLP, 88 Black Falcon Avenue, Boston, MA 02210 (US).

(81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European

(54) Title: METHOD AND SYSTEM FOR MANAGING CREDENTIALS

200

RESOURCE: "112"   ~ 202

ALICE IS PERMITTED ACCESS   ~ 204

205 — CLIENT x 1 IS PERMITTED ACCESS

206 — CLIENT x 2 IS PERMITTED ACCESS

208 — GROUP G1 IS PERMITTED ACCESS

210 — GROUP G2 IS PERMITTED ACCESS

212 — GROUP GN IS PERMITTED ACCESS

ACL OF RESOURCE ON SERVER BOB

(57) Abstract: The basic concept is that before a resource is accessed, the entity that has the burden of gathering the credentials, pro-actively refreshes the credentials and keeps them current. In one instance, a presenter of credentials, for example, a client pro-actively refreshes the credentials such that at the time of presentation, the credentials meet the resource-specific constraints of a recipient of credentials, for example, a resource server. For each resource that it protects, a resource server typically establishes various constraints such as a recency requirement, which specifies how recently a credential has to have been issued to be accepted as an adequate credential. Other constraints may include maximum certificate chain length, trust level and so forth. In another instance, a recipient of credentials pro-actively gathers and refreshes credentials to prevent un-authorized access to the various resources it is protecting.

WO 01/077797 A3